UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
(CHARLESTON DIVISION)

COTY MARTIN, Individually on behalf of Minor Child and on behalf of all others similarly situated,	:	
NICOLE ESCALERA, Individually and on on behalf all others similarly situated,	:	
Plaintiffs,	:	**CIVIL ACTION NO.:**
v.	:	**2:20-CV-03286-RMG**
BLACKBAUD, INC.,	:	
Defendant.	:	

AMENDED CLASS ACTION COMPLAINT

1. Plaintiff Coty Martin, on behalf of Minor Child and all others similarly situated, ("Plaintiff Martin") and Plaintiff Nicole Escalera, individually and on behalf of all others similarly situated ("Plaintiff Escalera") (collectively, "Plaintiffs") bring this action against Defendant Blackbaud, Inc. ("Blackbaud" or "Defendant") seeking monetary damages, restitution, and/or injunctive relief for the Class, as defined below. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

2. Blackbaud is a software company based in Charleston County, South Carolina. Between February 7, 2020 and May 20, 2020, cyber criminals orchestrated what Blackbaud called a "ransomware incident" by infiltrating the inadequately protected computer networks maintained by Blackbaud, thereby gaining access to and copying data and servers managed, maintained and

secured by Blackbaud. ("Data Breach"). In a ransomware attack, typically one is "locked out" of one's data or system by a malicious actor until a ransom is paid. Once the ransom is paid, access is granted. That is not all that happened here. Cyber criminals successfully breached Blackbaud's network and exfiltrated data from it. Blackbaud admitted to having data exfiltrated during the "ransomware incident," as evidenced by its filing to the SEC on September 29, 2020: "further forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords."

3. Blackbaud's servers contained Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively "Private Information"), of individual consumers, the Plaintiffs here. As a result of this Data Breach, Plaintiffs suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. Additionally, Plaintiffs and Class Members' sensitive Private Information—which was entrusted to Defendant—was not only compromised and unlawfully accessed due to the Data Breach and subject to unlawful use by unknown parties, but also prompted Plaintiffs and Class Members to purchase mitigating protective services. Information compromised in the Data Breach included a "copy of a subset of information" retained by Blackbaud, including name(s), addresses, phone numbers, and other Personally Identifiable Information and Protected Health Information.

4. True and accurate copies of the notices of data breach emailed to Plaintiffs (collectively "Notices") are attached hereto as Exhibits A and B, and Defendant's exemplar Notice is available on its website.[1] Contrary to the representations in the Notices by Blackbaud or its

[1] https://www.blackbaud.com/securityincident (Last Accessed August 12, 2020).

clients, Social Security Numbers, credit card numbers, bank account numbers, and Private Information have been compromised. *Id.*

5. Plaintiffs bring this class action lawsuit in order to, (1) address Defendant's inadequate safeguarding of Class Members' Private Information, which Defendant managed, maintained, and secured; (2) address Defendant's failure to provide timely and adequate notice to Plaintiffs that their information had been subject to the unauthorized access of an unknown third-party; (3) address Defendant's failure to identify all information that was accessed; and (4) address Defendant's failure to provide Plaintiffs with any redress for the Data Breach or act to mitigate their damages.

6. Defendant caused substantial harm and injuries to Plaintiffs across the United States by, *inter alia*, failing to: (1) timely implement adequate and reasonable measures to ensure Plaintiffs' Private Information was properly protected; (2) timely detect the Data Breach; (3) take adequate steps to prevent and stop the Data Breach; (4) disclose the material facts that it did not have adequate systems and security practices to safeguard Private Information; (5) honor its repeated promises and representations to protect the Plaintiffs' Personally Identifiable Information and Protected Health Information; (6) identify all information that was accessed; (7) maintain its computer network in a condition to adequately protect against ransomware attacks or other cyberattacks; (8) provide timely and adequate notice of the Data Breach; (9) properly monitor the computer network and systems that housed Breach Victims' Private Information; (10) implement appropriate policies to ensure secure communications; (11) properly train employees regarding ransomware attacks; and (12) provide Plaintiffs with any redress for the Data Breach.

7. Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information; failed to implement appropriate policies to ensure secure communications; and failed to properly train employees regarding ransomware attacks. Had Defendant properly monitored its network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether. In fact, Blackbaud has announced it has "already implemented changes to prevent this specific issue from happening again."[2] Had the necessary changes been made previously, this incident would not have happened and Plaintiffs' Private Information would not have been accessed.

8. Plaintiffs' identities and Private Information are now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained was in the hands of data thieves. Defendant cannot reasonably maintain that the data thieves destroyed the subset copy simply because Defendant paid the ransom and the data thieves confirmed the copy was destroyed. In fact, Defendants notices advise the affected individuals to monitor their own credit, beware of suspicious account activity, and notify the school or non-profit of suspicious activity related to his or her credit. Despite this, Defendant has not offered any manner of redress, including, *inter alia*, credit monitoring.

9. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using Class Members' names to obtain medical services, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names (but with another person's photograph) and giving false information to police during an arrest.

[2] https://www.blackbaud.com/securityincident (Last Accessed August 12, 2020).

10. As a result of the Data Breach, Plaintiffs and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members, at their own cost, must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Consequently, Plaintiffs and Class Members will also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly-situated individuals, whose Private Information was accessed during the Data Breach.

13. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

14. Accordingly, Plaintiffs bring this action against Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) intrusion upon seclusion or common law breach of privacy, (iii) negligence *per se,* (iv) breach of implied contract, and (vi) violations of South Carolina and California state data breach statutes.

PARTIES

15. Plaintiff Coty Martin is a resident and citizen of Garner, Johnston County, North Carolina. Plaintiff Martin is acting as the parent and guardian of Minor Child on his own behalf and on behalf of others similarly situated. Plaintiff Martin's Minor Child's Personally Identifiable Information and Protected Health Information was breached during the Blackbaud Data Breach.

16. Plaintiff Nicole Escalera is a resident and citizen of Fresno, Fresno County, California. Plaintiff Escalera is acting in her personal capacity and on behalf of others similarly situated. Plaintiff Escalera received notice of the breach on September 10, 2020. Plaintiff Escalera's Private Information was breached, and she has been the victim of attempted identity theft.

17. Defendant Blackbaud is a Delaware corporation with its principal place of business located on Daniel Island, Charleston County, South Carolina.

18. Defendant manages, maintains, and provides cybersecurity for the data obtained by its clients who are, *inter alia*, hospitals, non-profit companies and schools, which maintained Plaintiffs' PII and Plaintiffs' PHI – the data that was breached in this instance.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

20. This Court has personal jurisdiction over this action because Defendant maintains its principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District. This Court also has diversity jurisdiction over this action. 28 U.S.C. § 1332(a).

21. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant resides in this District.

DEFENDANT

22. Since originally incorporating in 1982,[3] Blackbaud has become "the world's leading cloud software company powering social good." This includes providing its clients with "cloud software, services, expertise, and data intelligence…" Blackbaud is a publicly traded company with clients that include "nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them."[4]

23. In 2019, Blackbaud reported that it had "45,000 customers located in over 100 countries," with a "total addressable market (TAM)… greater than $10 billion."[5]

24. In the ordinary course of doing business with Defendant's clients, individuals are regularly required to provide Defendant's clients with sensitive, personal and private information that is then stored, maintained, and secured by Defendant. This Private Information includes or may include the following personal data:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security numbers;
- Credit card account numbers;
- Bank account numbers;
- Educational history;
- Healthcare records or other HIPAA protected data;

[3] https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417 (Last Accessed August 12, 2020).
[4] https://www.blackbaud.com/company (Last Accessed August 12, 2020).
[5] https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417 (Last Accessed August 12, 2020).

- Insurance information and coverage;
- Photo identification;
- Employer information;
- Income information;
- Donor contribution information; and
- Addresses, place of birth, mother's maiden names, passwords or other Private Information.

25. At all relevant times, Blackbaud knew the data it stores was vulnerable to cyber-attack. In its 2019 Annual Report, Blackbaud specifically admits its known susceptibility to cyberattacks. Specifically, Blackbaud states,

> If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer.
>
> Fundamental to the use of our solutions is the secure collection, storage and transmission of confidential donor and end user data and transaction data, including in our payment services. Despite the network and application security, internal control measures, and physical security procedures we employ to safeguard our systems, we may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data, which may harm our business, reputation and future financial results.
>
> Like many major businesses, we are, from time to time, a target of cyber-attacks and phishing schemes, and we expect these threats to continue.
>
> Because of the numerous and evolving cybersecurity threats, including advanced and persistent cyber-attacks, phishing and social engineering schemes, used to obtain unauthorized access, disable or degrade systems have become increasingly more complex and sophisticated and may be difficult to detect for periods of time, we may not anticipate these acts or respond adequately or timely...[6]

[6] https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417 (Last Accessed August 10, 2020).

26. Because of the highly sensitive and personal nature of the Private Information Defendant maintains, manages, and secures with respect to its "end users" of its clients, the Plaintiffs here, Defendant has publicly affirmed its obligation and duty to secure their data.

27. Blackbaud's Privacy Policy North America ("Privacy Policy") expressly states:

> At Blackbaud, we are committed to protecting your privacy. This Policy applies to Blackbaud's collection and use of personal data in connection with our marketing and provision of the Blackbaud Solutions, customer support and other services (collectively, the "Services"), for example if you are a customer, visit the website, interact with us at industry conferences, or work for a current or prospective customer of the Services.

28. Defendant represents with regard to the security of personal information:

> We restrict access to personal information collected about you at our website to our employees, our affiliates' employees, those who are otherwise specified in this Policy or others who need to know that information to provide the Services to you or in the course of conducting our business operations or activities. While no website can guarantee exhaustive security, we maintain appropriate physical, electronic and procedural safeguards to protect your personal information collected via the website. We protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons.
>
> We also advise all Blackbaud employees about their responsibility to protect customer data and we provide them with appropriate guidelines for adhering to our company's business ethics standards and confidentiality policies. Inside Blackbaud, data is stored in password-controlled servers with limited access.[7]

29. Blackbaud professes that its privacy policy is somehow supplanted by its clients:

> If you're a constituent, supporter, patient or student of one of our customers, to which we provide the Services, your data will be used in accordance with that customer's privacy policy. In providing the Services, Blackbaud acts as a service provider and thus, this Policy will not apply to constituents of our customers.[8]

[7] *Id.*
[8] https://www.blackbaud.com/company/privacy-policy/north-america (Last Accessed August 12, 2020).

30. Blackbaud cannot absolve itself from its obligation or duty based on assertion of a lack of privity, having already pointed out in a recent SEC filing that "plaintiffs lack contractual privity with us."[9]

31. The duty to Protect the Private Information is non-delegable, particularly here where Blackbaud's entire business model is premised upon voluntarily assuming that duty via soliciting customers to utilize its professed ability to manage, house and safeguard data. Plaintiffs allege that under any privacy policy, Blackbaud is liable for the removal of this data.

32. In fact, children's data is particularly attractive to data thieves and can have long-lasting effects on the child's financial history and identity. Specifically,

> theft of a child's identity is lucrative to a cyber-criminal because it can remain undetected for years, if not decades. Without regular monitoring, a child's identity that has been stolen may not be discovered until they are preparing to go to college and start applying for student loans or get their first credit card. By then, the damage is done and the now young adult will need to go through the pain of proving that their identity was indeed stolen.[10]

33. In 2011, Carnegie Mellon University's CyLab reported "the rate of child identity theft is 51 times higher than for adults (whose data sets cost about $10 - $25 on dark web markets)."[11]

34. By early 2018, it became well known that the data of infants was being sold on the dark web. As of 2018, the cost of an infant's data was approximately $300 in bitcoin, which would "provide cybercriminals access to a clean credit history."[12]

---

[9] https://investor.blackbaud.com/static-files/b861e404-fa85-4f5b-a833-bc30de0165dd (Last Accessed November 6, 2020)
[10] https://axiomcyber.com/data-breach/how-data-breaches-affect-children/ (Last Accessed November 10, 2020).
[11] https://money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html (Last Accessed November 10, 2020).
[12] *Id.*

35. As instructed by the Federal Trade Commission,

> A child's Social Security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live. [13]

36. As one cyber security author further explained, the impact of the use of children's information is further exacerbated by the fact that there are few checks on using a child's data to initially obtain credit and slowly increase it over time- all while being undetected by the child and the parents.[14] Thus, "[t]he problem goes unnoticed for years — possibly decades — before the child goes to apply for student loans, open their first credit card, or buy their first car."[15]

37. While regulations about how children's personal information is collected and maintained, the companies providing the service of collecting and maintaining claim to understand this critical concern about the safe keeping of children's data.

38. In fact, Blackbaud has made further commitments to the maintenance of student's private information. In April of 2015 with re to its K-12 school providers, Defendant signed a pledge to respect student data privacy to safeguard student information. The Student Privacy Pledge, developed by the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA), was created to "safeguard student privacy in the collection, maintenance and use of personal information."[16]

39. In signing the Student Privacy Pledge, Blackbaud specifically represented to students and parents of its K-12 school providers that it would, *inter alia*, (1) "[m]aintain a

---

[13] https://www.consumer.ftc.gov/articles/0040-child-identity-theft (Last Accessed November 12, 2020).
[14] https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/ (Last Accessed November 12, 2020).
[15] *Id.*
[16] https://www.blackbaud.com/home/2015/04/22/blackbaud-signs-pledge-to-respect-student-data-privacy (Last Accessed October 12, 2020).

comprehensive security program:" and (2) "[b]e transparent about collection and use of student data."[17]

40. In further support of this representation and promise to student and parent users, Travis Warrant, president of Blackbaud's K-12 Private Schools Group, stated:

> Blackbaud is committed to protecting sensitive student data and security… The Pledge will better inform our customers, service providers and the general public of our dedication to protecting student privacy." The Pledge details ongoing industry practices that meet (and in some cases, exceed) all federal requirements, and encourages service providers to more clearly articulate their data privacy practices.[18]

41. Despite its duties, representations and promises, Defendant failed to adequately secure and protect numerous K-12 providers and thousands of students Private Information, by allowing the Private Information to be copied and potentially used or sold at a later date.

42. Further, due to the Health Information Portability and Accountability Act (HIPAA), Defendant had additional obligations to secure patient users' information for healthcare Clients.

43. Defendant has further failed Plaintiffs and Class Members by failing to adequately secure and protect their PII and PHI, by allowing the PII and PHI to be copied and potentially used or sold at a later date.

44. Defendant further failed Plaintiffs and Class Members by failing to adequately notify them of the ransomware attack and resulting Data Breach or provide any remedy other than belated and facially inadequate notice.

THE DATA BREACH

45. Prior to the ransomware attack and data breach, Plaintiffs provided sensitive and identifying Private Information to Blackbaud as part of, *inter alia*, seeking healthcare from

[17] *Id.*
[18] *Id.*

healthcare providers; making donations to non-profit companies; seeking education from K-12 school providers and universities; or in seeking other services from Blackbaud's clients. When providing such information, these individuals had the expectation that Defendant, as the manager and securer of this Private Information, would maintain security against cybercriminals and cyberattacks.

46. Defendant maintained Plaintiffs' data on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks on health care, schools, and other facilities over the course of recent years, Defendant did not maintain adequate security of Plaintiffs' data, or adequately protect against hackers and cyberattacks.

47. According to its own statements, posted to its website in July 2020, Defendant initially discovered a ransomware attack in May of 2020. The attack attempted to "disrupt business by locking companies out of their own data and servers."[19] According to Defendant's statements:

> After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly… The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.[20]

[19] https://www.blackbaud.com/securityincident (Last Accessed August 12, 2020).
[20] *Id.*

48. The ransomware attack that began in February of 2020 and continued until May of 2020 led to the removal of a copy of the data.

49. Although Defendant claims that social security numbers, credit card information, or bank account information was not accessed, the Notices advise individuals whose PII and PHI was accessed to, *inter alia*, "carefully review the bills you receive from your healthcare providers." Exhibits A and B. Defendant's statements of reassurance were unfounded in light of their later admission to the SEC: "further forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords."[21]

50. Defendant did not have a sufficient process or policies in place to prevent cyberattack and access, which is evident by its own statements that it has "already implemented changes to prevent this specific issue from happening again."[22]

51. The acknowledged types of data exposed included patient's PII and PHI, such as patient's name, address, phone number(s), email address, date of birth, room number, patient identification number, the name of the hospital where [they] were treated and the name of the treating physician. Exhibits A and B. Plaintiffs were also instructed to "carefully review bills you receive from your healthcare providers" and "proactively monitor account statements, bills and notices for any unusual activity." Exhibits A and B.

52. Defendant should not be allowed to reasonably rely on the word of data thieves or cyber criminals that the "copied" or stolen subset of any data was destroyed. Defendant has not

[21] Blackbaud, Inc. filing with the U.S. Securities and Exchange Commission (9/29/2020); https://www.sec.gov/ix?doc=/Archives/edgar/data/1280058/000128005820000044/blkb-20200929.htm.

[22] https://www.blackbaud.com/securityincident (Last Accessed August 12, 2020).

and cannot be assured that Social Security numbers, Bank Account numbers, and Credit Card numbers were not also accessed and retained by the data thieves, or it would not have advised its clients to advise affected individuals to monitor accounts for suspicious activity. Despite recognizing the need for monitoring due to significant heightened risk, Defendant has failed to offer its clients or their users any mitigation or remedy, including credit monitoring.

53. Despite having knowledge of the attack and compromised stolen data since at least May 2020, Defendant willfully and knowingly withheld this knowledge from its affected clients until July or August 2020.

54. Defendant has obligations and duties created by state and federal law, contracts, industry standards, common law, and privacy representations made to Plaintiffs to keep their PII and PHI secure, confidential and to protect it from unauthorized access and disclosure.

55. Plaintiffs provided their PII and PHI to Defendant or Defendant's client with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

56. Defendant's duty to secure their data was not only non-delegable, but it also was particularly important given the substantial increase in cyberattacks and/or data breaches in its client's various industries preceding the date of the data breach.

57. Indeed, cyberattacks have become so notorious that as recently as November 2019, the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issued warnings to potential targets like Blackbaud so they are aware of, and prepared for, a potential attack. [23]

[23] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (emphasis added) (Last Accessed August 12, 2020).

58. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including by Defendant's own admissions in its 2019 Annual Report.

59. Defendant breached its obligations to Plaintiffs and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Defendant's computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to timely notify its Clients, Plaintiffs, and Class Members of the data breach; and

e. In other such ways yet to be discovered.

60. As the result of Defendant's failure to take certain measures to prevent the attack until after the attack occurred, Defendant negligently and unlawfully failed to safeguard Plaintiffs' Personally Identifiable Information and Protected Health Information.

61. Accordingly, as outlined below, Plaintiffs' daily lives were disrupted, Plaintiff Escalera was victimized by attempted identity theft, and Plaintiffs and Class Members face an increased risk of fraud and identity theft.

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

62. Cyberattacks and data breaches of medical facilities, schools, and non-profit entities are especially problematic because of the disruption they cause to the overall daily lives of individuals affected by the attack.

63. Perhaps most illustrative of the danger that can be caused by cyberattacks on medical facilities, the first known death from a cyberattack was recently reported in Germany after a ransomware attack crippled a hospital's systems and they were forced to turn away emergency patients.[24]

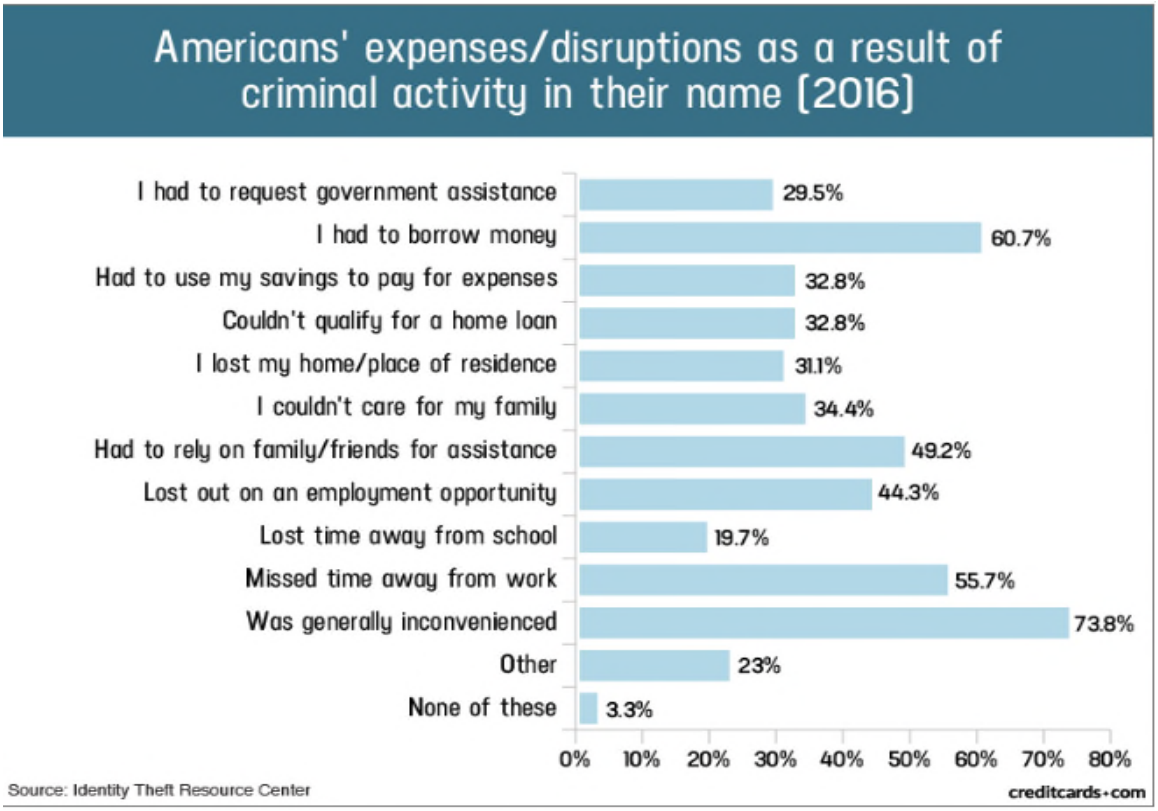
64. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

65. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[26]

66. Cyber criminals use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

[24] https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (Last Accessed on November 3, 2020).
[25] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").
[26] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

67. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name, but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[27]



[27] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited August 12, 2020).

68. Personally Identifiable Information is a valuable property right.[28] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. This obvious risk to reward analysis illustrates that Personally Identifiable Information and Protected Health Information have considerable market value that is diminished when it is compromised.

69. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

70. Personally Identifiable Information is such an inherently valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

71. There is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning Plaintiffs are at an increased risk of fraud and identity theft for many years into the future. Thus, as the Notices advise, Plaintiffs must vigilantly monitor their financial and medical accounts for many years to come. *See* Exhibits A and B.

[28] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

72. To date, Defendant has done nothing to provide Plaintiffs with relief for the damages they have suffered as a result of the Data Breach including, but not limited to, the costs of credit monitoring, as well as costs and loss of time they incurred because of the data breach.

73. Plaintiffs and Class Members have been damaged by the compromise of their Personally Identifiable Information in the Data Breach.

74. The Personally Identifiable Information and Protected Health Information of Plaintiff Coty Martin's Minor Child was compromised as a direct and proximate result of the Data Breach. While the compromise of this information was known as early as May of 2020, Plaintiff Martin did not receive Notice until August 30, 2020. Exhibit A.

75. Specifically, Plaintiff Coty Martin's Minor Child, now 11 years old, had undergone more than a year of care at the Atrium Health hospital where the data was compromised. Included in the compromised PHI were dates of treatment, location of services, and the treating physician's name. The physician's name alone could easily be researched to discover that the Minor Child was treated by, among others, an oncologist. Knowing that an oncologist treated the Minor Child necessarily reveals that he had cancer.

76. The exposure of all of the Minor Child's treating physician's names, as well as duration of treatment, and the resulting information that could be obtained therefrom, could create obstacles for the Minor Child in the future, including social stigmas, the inability to obtain a job, or other difficulties associated with having endured a prolonged illness.

77. That Blackbaud's Grateful Patient platform was used to take the most sensitive PHI of a child, during the most difficult period of his life (and his parents' lives), and that Blackbaud

failed to adequately secure that data has caused and will cause significant damage to the Minor Child.

78. Consequently, even utilizing credit monitoring, data thieves could conceivably wait another seven or more years to sell or use the Minor Child's information without detection. Thus, the Minor Child will require more than the average seven years of credit monitoring to ensure that his identity will not be compromised as a result of this Data Breach.

79. Further, even if the Minor Child's credit is frozen, he will eventually need to unfreeze his credit to build credit, obtain a car loan, obtain a mortgage, and various other tasks that begin when a child turns 18 years old. Doing so will make him vulnerable again in the future.

80. The Personally Identifiable Information and Protected Health Information of Plaintiff Nicole Escalera was compromised as a direct and proximate result of the Data Breach. While the compromise of this information was known as early as May 2020, Plaintiff Escalera did not receive Notice until September 8, 2020. Exhibit B.

81. As a result of the Data Breach, Plaintiff Escalera must frequently monitor her credit for suspicious activity. In doing so, Plaintiff Escalera recently discovered and reported an unauthorized account opened in her name in November 2020 with an electric company in California.

82. Like Plaintiffs, other Class Members' Private Information and Private Health Information was compromised as a direct and proximate result of the Data Breach.

83. As a direct and proximate result of Defendant's conduct, Plaintiffs have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

84. As a direct and proximate result of Defendant's conduct, Plaintiffs have been forced to expend time dealing with the effects of the Data Breach.

85. Plaintiffs face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

86. Plaintiffs face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII and PHI as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs.

87. Plaintiffs have also incurred out-of-pocket costs for protective measures such as credit monitoring fees, and may also incur additional costs for credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

88. Plaintiffs also suffered a loss of value of their PII and PHI when it was removed and acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in such cases.

89. Plaintiffs have spent and will continue to spend significant amounts of time to respond to the data breach and monitor their financial, student, and/or medical accounts and records for misuse.

90. Plaintiffs have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiffs suffered ascertainable losses in the form of out-of-pocket expenses, loss of the value of their time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come; and

l. Interacting with government agencies and law enforcement to address the impact and harm caused by thid breach.

91. Moreover, Plaintiffs have an interest in ensuring that their PII and PHI, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing their data is not accessible online and that access to such data is limited and secured.

92. As a result of Defendant's failures to safeguard Plaintiffs' data, Plaintiffs are forced to live with the knowledge that their Personally Identifiable Information or Private Health Information—which contains many private and intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment, loss of security and depriving them of their fundamental right to privacy.

93. As many of the purchasers of Private Information or Private Health Information may not utilize the stolen information immediately, Plaintiffs will be forced for long periods of time to endure the fear of whether and how their information will be used against them.

94. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of harm.

CLASS ACTION ALLEGATIONS

95. Plaintiff Coty Martin brings this action on behalf of Minor Child and on behalf of all natural persons similarly situated.

96. Plaintiff Nicole Escalera brings this action on her own behalf and on behalf of all natural persons similarly situated.

97. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> Nationwide Class: All natural persons residing in the United States whose Private Information (PII) or Private Health Information (PHI) was compromised as a result of the Blackbaud data breach.

98. Plaintiffs also propose the following Subclass definitions, subject to amendment as appropriate:

> South Carolina Subclass: All natural persons residing in South Carolina whose Private Information (PII) or Private Health Information (PHI) was compromised as a result of the Blackbaud data breach.
>
> California Subclass: All natural persons residing in California whose Private Information (PII) or Private Health Information (PHI) was compromised as a result of the Blackbaud data breach.

The South Carolina Subclass includes Plaintiff Martin. The California Subclass includes Plaintiff Escalera. Excluded from the Class and subclasses are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal

representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class and subclasses are members of the judiciary to whom this case is assigned, their families and members of their staff.

99. Numerosity. The members of the Class (and subclasses) are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, the class consists of approximately hundreds of thousands of persons and entities whose data was compromised in the Data Breach.

100. Commonality. There are questions of law and fact common to Plaintiffs and the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information and/or Private Health Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Personally Identifiable Information and/or their Protected Health Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Personally Identifiable Information and /or their Protected Health Information;

g. Whether computer hackers obtained, sold, copied, stored or released Class Members' Personally Identifiable Information and/or Protected Health Information;

h. Whether Defendant knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether Plaintiffs suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

101. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

102. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

103. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all Plaintiffs' and Class Members' data at issue here was stored on the same computer systems and allowed to be unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

104. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

105. Defendant has acted on grounds that apply generally to the Class (and subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

FOR A FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs, the Nationwide Class and All Subclass Members)

106. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 104 above, as if fully set forth herein.

107. Defendant's Clients required Plaintiffs and Class Members to submit non-public personal information in order to obtain medical, educational, and other services. Defendant had a duty to Class Members to securely maintain the PII and PHI collected as promised and warranted.

108. By voluntarily accepting the duty to maintain and secure this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer systems—and Plaintiffs' PII and PHI held

within it—to prevent disclosure of the information, and to safeguard the information from cyber theft. Defendant's duty included a responsibility to implement processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt notice to those affected by a data breach and/or ransomware attack.

109. Defendant owed a duty of care to Plaintiffs to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected and safeguarded the PII and PHI of the Class.

110. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its Clients' End Users (the Class here), which is recognized by Defendant's Privacy Policy, as well as applicable laws and regulations. Defendant actively solicited Private Information as part of its business and was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a ransomware attack and resulting data breach.

111. Defendant had a specific duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

112. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

113. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' data. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Personally Identifiable Information and/or Protected Health Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Personally Identifiable Information and/or Protected Health Information;

e. Failing to detect in a timely manner that Class Members' Personally Identifiable Information and/or Protected Health Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach and Ransomware Attack so those put at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages.

114. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII and PHI would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

115. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII and PHI would result in one or more types of injuries to Class Members.

116. Plaintiffs are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

117. Plaintiffs are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members, and any other relief this count deems just and proper.

FOR A SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs, the Nationwide Class and All Subclass Members)

118. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 116 above, as if fully set forth herein.

119. When Plaintiffs and Class Members provided their Personally Identifiable Information or Protected Health Information to Defendant and Defendant's Clients in exchange for Defendant and Defendant's Clients' services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

120. Defendant solicited and invited Class Members to provide their Personally Identifiable Information or Protected Health Information as part of Defendant's regular business practices, including through its Privacy Policy. Plaintiffs and Class Members accepted Defendant's offers and provided their data to Defendant.

121. In entering into such implied contracts, Plaintiffs reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

122. Plaintiffs accepted service from, and paid money to Defendant's Clients which was conferred upon Defendant, and through which Plaintiffs reasonably believed and expected that

Defendant would use part of those funds to maintain adequate data security. Defendant failed to do so.

123. Plaintiffs would not have entrusted their Personally Identifiable Information or Protected Health Information to Defendant in the absence of the implied contract between them and Defendant to keep that information secure. Plaintiffs would not have entrusted their Personally Identifiable Information or Protected Health Information to Defendant in the absence of their implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

124. Plaintiffs fully and adequately performed their obligations under the implied contracts with Defendant.

125. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their data.

126. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

127. Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

128. Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOR A THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs, the Nationwide Class and All Subclass Members)

129. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 127, above as if fully set forth herein.

130. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

131. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' Private Information.

132. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

133. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

134. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' data would not have been stolen and they would not have been harmed.

135. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personally Identifiable Information or Protected Health Information, including increased risk of identity theft.

136. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOR A FOURTH CAUSE OF ACTION
WRONGFUL INTRUSION INTO PRIVATE AFFAIRS/INVASION OF PRIVACY
(On Behalf of Plaintiff Martin and the South Carolina Subclass Members)

137. Plaintiff Martin repeats and re-alleges each and every allegation contained in Paragraphs 1 through 135, as if fully set forth herein.

138. The State of South Carolina recognizes the tort of wrongful intrusion, and the South Carolina Supreme Court has indicated that it consists of a "wrongful intrusion into one's private activities, in such manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities." *O'Shea v. Lesser*, 416 S.E.2d 629, 633 (S.C. 1992) (quoting *Meetze v. The Associated Press*, 95 S.E.2d 606 (S.C. 1956)).

139. Plaintiffs here had a reasonable expectation of privacy, and freedom from exposure, in the data Defendant mishandled.

140. Defendant's conduct as alleged above intruded upon Plaintiffs private activities under common law.

141. Defendant's intrusion was substantial and unreasonable enough to be legally cognizable, in that the reasonable expectation of persons of normal and ordinary sensibilities, including Plaintiffs, is that the Personally Identifiable Information or Protected Health Information entrusted to Defendant's Clients would be properly maintained and secured.

142. By failing to keep Plaintiffs' and Class Members' Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally or negligently publicizing private facts about Plaintiffs and Class Members, which is offensive and objectionable to an ordinary person; and

c. Intentionally or negligently causing anguish or suffering to Plaintiffs and Class Members.

143. Defendant knew that an ordinary person in Plaintiffs' or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

144. Defendant invaded Class Members' right to privacy and intruded into Plaintiffs' private lives and affairs by intentionally misusing and/or disclosing their Personally Identifiable Information or Protected Heath Information without their informed, voluntary, affirmative, and clear consent.

145. Defendant intentionally concealed from Plaintiffs the ransomware attack that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

146. As a proximate result of such intentional misuse and disclosures, Plaintiffs' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

147. In failing to protect Plaintiffs' Personally Identifiable Information or Protected Health Information, and in intentionally misusing and/or disclosing their data, failing to properly

notify the Class, Defendant acted with intent and in conscious disregard of Plaintiffs' and Class Members' privacy rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

FOR A FIFTH CAUSE OF ACTION
VIOLATION OF STATE DATA BREACH STATUTES
(On Behalf of Plaintiff Martin and the South Carolina Subclass Members)

148. Plaintiff Martin re-alleges and incorporates by reference Paragraphs 1 through 146 above, as if fully set forth herein.

149. Defendant owns, licenses and/or maintains computerized data that includes Plaintiff Martin's and the South Carolina Subclass Members' Personally Identifiable Information or Protected Health Information.

150. Defendant's conduct, as alleged above, violated the data breach statutes of South Carolina, including, S.C. Code § 1-11-490 (2008) and/or S.C. Code § 39-1-90 (2009) (the "State Data Breach Acts").

151. Defendant was required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber security incident described herein.

152. The Data Breach constituted a "breach of the security system" within the meaning of the State Data Breach Acts.

153. The information compromised in the Data Breach constituted "personal identifying information" within the meaning of the State Data Breach Acts, and Protected Health Information under HIPAA.

154. The State Data Breach Acts require disclosure of data breaches "in the most expedient time possible and without unreasonable delay…."

155. Defendant violated the State Data Breach Acts by unreasonably, willfully, and knowingly delaying disclosure of the Data Breach to Plaintiff Martin and other South Carolina Subclass Members, whose Personally Identifiable Information was, or was reasonably believed to have been, acquired by an unauthorized person.

156. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiff Martin and the South Carolina Subclass Members would impede a criminal investigation.

157. As a result of Defendant's violation of the State Data Breach Acts, Plaintiff Martin and the South Carolina Subclass Members incurred harm and seek damages as alleged herein.

158. Plaintiff Martin, on behalf of Minor Child and on behalf of the South Carolina Subclass, seeks all remedies available under the State Data Breach Acts, including, but not limited to: (a) actual damages suffered by the South Carolina Subclass Members as alleged above; (b) statutory damages for Defendant's willful, intentional, and/or reckless conduct; (c) equitable relief; and (d) reasonable attorneys' fees and costs.

FOR A SIXTH CAUSE OF ACTION
INVASION OF PRIVACY AND VIOLATION OF THE CALIFORNIA CONSTITUTION
Art. 1, § 1
(On Behalf of Plaintiff Escalera and the California Subclass Members)

159. Plaintiff Escalera re-alleges and incorporates by reference Paragraphs 1 through 157 above, as if fully set forth herein.

160. Plaintiff Escalera and the California Subclass members have a legally protected privacy interest in their Personally Identifiable Information or Protected Health Information that

is transferred to or recorded by Blackbaud, and are entitled to the protection of their property, data and information against unauthorized access.

161. Plaintiff Escalera and the California Subclass members reasonably expected that their personal data would be protected and secure from unauthorized parties, and that their Personally Identifiable Information or Protected Health Information would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

162. Defendant unlawfully invaded the privacy rights of Plaintiff Escalera and the California Subclass members by (a) failing to adequately secure their Personally Identifiable Information or Protected Health Information from disclosure to unauthorized parties for improper purposes; (b) disclosing their Personally Identifiable Information or Protected Information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their Personally Identifiable Information or Protected Health Information to unauthorized parties without the informed and clear consent of Plaintiff Escalera and the California Subclass members, including but not limited to the Blackbaud Data Breach. This invasion into the privacy interests of Plaintiff Escalera and the California Subclass members is serious and substantial.

163. In failing to adequately secure Plaintiff Escalera's and the California Subclass members' data, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its substandard security measures would cause harm, and would be considered highly offensive to a reasonable person in the same position as Plaintiff Escalera and the California Subclass.

164. Defendant violated Plaintiff Escalera's and the California Subclass members' right to privacy under California law, including, but not limited to, Article 1, Section 1 of the California Constitution and the California Consumer Privacy Act.

165. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiff Escalera and the California Subclass members' data has been accessed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff Escalera and the proposed California Subclass members have suffered injuries as a result of Defendant's unlawful invasions of privacy and are entitled to relief.

166. Plaintiff Escalera and the California Subclass members are entitled to injunctive relief as well as actual and punitive damages.

FOR A SEVENTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT,
Cal. Civ. Code § 1798.100, *et seq.*
(On Behalf of Plaintiff Escalera and the California Subclass Members)

167. Plaintiff Escalera re-alleges and incorporates by reference Paragraphs 1 through 165 above, as if fully set forth herein.

168. California's Consumer Privacy Act ("CCPA") recently was enacted to protect consumers' Personally Identifiable Information or Protected Health Information from "an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." *See* Cal. Civ. Code § 1798.150(a)(1)

169. Defendant was required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature of the information compromised in the Data Breach described herein.

170. The Data Breach constituted an "exfiltration, theft, or disclosure" within the meaning of the CCPA.

171. The information compromised in the Data Breach constituted "personal information" within the meaning of the CCPA and Cal. Civ. Code §§ 1798.80(e) and 1798.81.5(d)(1)(A).

172. Defendant violated the CCPA by failing to "implement and maintain reasonable security procedures and practices – to protect the personal information" of the Plaintiff Escalera and the California Subclass Members, whose Personally Identifiable Information or Protected Health Information was, or was reasonably believed to have been, "subject to an unauthorized access and exfiltration, theft, or disclosed as a result" of Defendant's violation of its duty.

173. In accordance with Cal Civ. Code § 1798.150(b), prior to the filing of this Complaint, Plaintiff Escalera's counsel served Defendant with notice of these CCPA violations by certified mail, return receipt requested.

174. Defendant Blackbaud acknowledged receipt of said notice and did not cure the alleged violation within the timeframe allowed by the CCPA.

175. Plaintiff Escalera, individually and on behalf of the California Subclass, seeks all remedies available under the CCPA, including, but not limited to: "(A) damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; (B) injunctive or declaratory relief; and (C) any other relief the court deems proper." *See* Cal. Civ. Code § 1798.150(a)(1).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Personally Identifiable Information or Protected Health Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members or to mitigate further harm;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personally Identifiable Information or Protected Health Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: December 7, 2020

Respectfully submitted,

MOTLEY RICE LLC

/s/ Jodi Westbrook Flowers
Jodi Westbrook Flowers (SC Bar No. 066300)
Temitope O. Leyimu (SC Bar No. 101288)
Andrew P. Arnold (SC Bar No. 102491)
C. Ross Heyl (SC Bar No. 104154)
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Tel: (843)216-9000
Fax: (843)216-9027
Email: jflowers@motleyrice.com
aarnold@motleyrice.com
tleyimu@motleyrice.com
rheyl@motleyrice.com

WHITFIELD BRYSON LLP

/s/ *Harper Todd Segui*
Harper Todd Segui (Fed ID No. 10841)
PO Box 1483
Mount Pleasant, SC 29465
Tel: (919) 600-5000
Fax: (919) 600-5035
Email: harper@whitfieldbryson.com

Alex Straus*
Matthew E. Lee*
Erin J. Ruben*
900 W. Morgan Street
Raleigh, NC 27603
T: 919-600-5000
Fax: 919-600-5035
Email: alex@whitfieldbryson.com
harper@whitfieldbryson.com
matt@whitfieldbryson.com
erin@whitfieldbryson.com

Attorneys for Plaintiffs and the Proposed Class
** Pro Hac Vice Applications Pending*

Exhibit A

Atrium Health

217 1 74316 **********AUTO**ALL FOR AADC 275
Parent or Guardian of:
BRAYTON MARTIN
1396 FIELDTRIAL CIR
GARNER, NC 27529-6540

August 28, 2020

Su información personal puede haber estado involucrada en un posible incidente cibernético. Si desea recibir una versión de esta carta en español, por favor llame 1-888-498-0914.

Dear Parent or Guardian of Brayton Martin,

Atrium Health is committed to improving health, elevating hope, and advancing healing – for all. We do this through many valuable initiatives, including offering new lifesaving services to the most vulnerable patients in our children's hospitals and increasing access to our world-class cancer network and other service lines. We could not accomplish this alone and are grateful for the many patients and donors who help us fulfill our mission.

To support our philanthropic efforts, we, like thousands of other non-profit, academic, and health care institutions across the country, use a relationship management software from a company called Blackbaud. On July 16, 2020, Blackbaud notified us that it discovered a ransomware attack on its systems that may have involved personal information belonging to some of our patients. While Blackbaud assures us that it has addressed the situation, we wanted to let you know what happened and share what has been done in response.

What Happened at Blackbaud?
On May 14, 2020, Blackbaud discovered that an unauthorized party accessed its systems. Blackbaud's investigation determined that the unauthorized access occurred from February 7, 2020 to May 20, 2020. Shortly after discovering the attack, Blackbaud locked the cybercriminals out of its systems. During the period of access, however, the cybercriminals were able to remove a copy of a back-up database that included information belonging to numerous Blackbaud clients. Unfortunately, Atrium Health was one of those clients.

What Did Blackbaud Do in Response?
Blackbaud paid the cybercriminals a ransom to delete the data. Blackbaud also hired a third-party firm to monitor for any misuse or public posting of the impacted dataset and indicates that it has not seen any evidence that the information still exists or is being misused. Finally, Blackbaud has confirmed it has identified and fixed the vulnerability associated with the incident and is accelerating its efforts to further protect the security of its environment through additional enhancements. To read more about Blackbaud's response, see www.blackbaud.com/securityincident.

What Information Was Affected?
Atrium Health takes privacy and security very seriously. As soon as we received notice from Blackbaud, we immediately began our own investigation to determine what, if any, personal information was potentially impacted. On August 12, 2020, we were able to determine that personal information belonging to your child may have been included in the affected back-up database at Blackbaud. Based on our review of the database, the personal information affected may have included your child's first and last name and contact information (such as home address, phone number and email), certain demographic information (including date of birth, guarantor information, and internally generated patient ID numbers), the dates of treatment, the locations of service, and the name of the treating physician. The information may also have included the name and relationship of your child's guarantor, such as a parent or guardian. If your child made a donation to support Atrium Health, the date and amount of the donation may have also been included.

What Information Was Not Affected?
It is important to note that the affected information did not include your child's Social Security number, credit card information or bank account information. Blackbaud does not and did not have any access to your child's medical record nor any information about your child's prognosis, medications, or test results.

What You Can Do

Although Social Security numbers, bank account and credit card information were not involved in this incident, we generally encourage individuals to proactively monitor their child's account statements, bills and notices for any unusual activity and to promptly report any concerns. Please consult the enclosed Reference Guide if you have any questions about how to obtain free credit reports, fraud alerts or security freezes, or need the contact information for the major credit bureaus.

What Atrium Health Is Doing

Even though this incident occurred solely at Blackbaud and not at Atrium Health, we are reviewing our own security safeguards as a precaution and remain vigilant for similar types of incidents. Please know that we take this matter very seriously and are reviewing our relationship with Blackbaud. We have also set up a call center that you can call toll-free at 1-888-498-0914 if you have questions or would like additional information. The call center is available Monday through Friday from 9am to 6:30pm Eastern Standard Time, excluding holidays.

We sincerely apologize for this incident at Blackbaud and any concern or inconvenience it may cause. We value our relationship with you and are honored to be able to provide care for you and your family.

Sincerely,

Atrium Health

Exhibit B

COMMUNITY
MEDICAL CENTERS

September 8, 2020

426 1 197940 ********** AUTO **5-DIGIT 93727
NICOLE ESCALERA
224 S CLOVIS AVE APT 126
FRESNO, CA 93727-4280

Dear Nicole Escalera,

Community Medical Centers ("Community") is committed to protecting the privacy of our patients and donors, and the security of their information. Regrettably, we have learned that Community is one of hundreds of hospitals, healthcare systems, and other nonprofit organizations, including several in California, to be affected by a security event at Blackbaud, the company that hosts our fundraising databases. This security incident involved some of your information.

Blackbaud is a vendor that provides Community with cloud-based, data solution services related to our donors and fundraising Foundation. Community maintains its electronic health record separate from the Foundation. On July 16, 2020, Blackbaud informed us that an unauthorized individual had gained access to Blackbaud's systems between February 7, 2020 and May 20, 2020. Blackbaud advised us that the individual may have acquired a backup of certain donor and prospective donor information, which sometimes included protected health information of our patients.

We immediately took steps to understand the extent of the incident and the data involved. Importantly, all Social Security numbers, bank account information and credit card numbers were encrypted, and therefore were **not** accessed. Also, this security incident did **not** involve access to any of Community's medical systems or our electronic health record system.

Based on information provided by Blackbaud, we believe that other confidential information was accessed by the unauthorized individual, and may have included: your name, address, phone number(s), email address, date of birth, room number, patient identification number, the name of the hospital where you were treated, and the applicable hospital department or unit.

We are taking this matter very seriously. To help prevent any future incidents such as this, Community is reviewing its relationship with Blackbaud and the specific security improvements that Blackbaud has now taken in response to this incident.

We deeply regret any concern or inconvenience this incident may cause and want you to know we value our relationship with you. We recommend you carefully review the bills you receive from your healthcare providers. If you see services you suspect you did not receive, please contact the provider immediately. Should you have questions, we have also established a dedicated call line for this incident at 1-866-968-0157, Monday through Friday, at 6 a.m. to 3:30 p.m. Pacific Time. When calling, please refer to Reference Number **YS1079504-P**.

Sincerely,

Debra A. Muscio, MBA, CFE, CCE, CHC, CHP, CHIAP
SVP, Chief Audit, ERM, Privacy, Information Security, Ethics and Compliance Officer
Community Medical Centers